Wireless Body Area Networks in Healthcare: Evolution, Challenges, and Pathways to Innovation

Jan Herbst[1], Jan Petershans[1], Seyedeh Ghazal Shobairian[1] and Hans Schotten[1,2]
[1]Intelligent Networks Research Group, German Research Center for Artificial Intelligence, Kaiserslautern, Germany
[2]Institute for Wireless Communication and Navigation, RPTU Kaiserslautern-Landau, Kaiserslautern, Germany

Jan.Herbst@dfki.de
Jan.Petershans@dfki.de
Seyedeh_ghazal.shobairian@dfki.de
schotten@rptu.de

Abstract: Wireless Body Area Networks (WBANs) are emerging as a transformative technology in healthcare, enabling continuous real-time monitoring, and management of patient health. This work explores the development of WBANs, emphasizing advances in communication standards such as Bluetooth, ZigBee, and Ultra-Wideband, alongside key challenges in their implementation. These challenges are categorized into five areas: i) security and privacy, ii) hardware, iii) communication and network protocols, iv) physiological aspects and v) interoperability. Additionally, the integration of WBANs into smart hospital environments as human-centric Internet-of-Things (IoT) systems is discussed, highlighting their potential to enhance patient care while addressing critical cybersecurity risks.

Keywords: Wireless body area networks (WBANs), Security and privacy, Communication rrameworks, Medical digital twin (MDT), Human-Centric IoT, Smart hospital

1. Introduction

In recent years, technological advancements across various sectors, particularly in healthcare and well-being, have significantly improved overall quality of life. This progress has not only been driven by innovations in information and communication technologies and interoperability, but also by forthcoming health monitoring systems. One particular area that has emerged is the field of Body Area Networks (BANs). Combining miniaturization and assembly techniques to facilitate the integration of electronic devices in or near the human body (Preethichandra *et al.*, 2023), the research and development of BANs can be traced back to 1961 with the Mackay Project for radio dust measurements (Mackay, 1959).

Building on these foundational concepts, the expansion to Wireless Body Area Network (WBAN) technologies in 1995 leveraged advancements in wireless personal area network technologies to provide communication capabilities for use on, near, or around the human body (Zimmerman, 1996; Yuce, 2010). Since then, WBANs have experienced increasing adoption in e-health systems, offering numerous benefits to patients and healthcare providers. The concept of WBANs requires small, self-programming nodes with low power consumption and flexible sensor capabilities, configured for processing and transmitting data to remote medical systems. Continuous monitoring and aggregation of physiological data via such devices provide valuable insights into health status for everyone from patients or athletes to healthcare professionals. This enables early detection of anomalies, personalized treatment planning, well-timed intervention, and improved patient recovery. Additionally, WBANs can reduce cost for healthcare and during treatment by enabling remote monitoring and real-time data transmission. This allows healthcare providers to assess patient status, offer objective advice, and facilitates informed decision-making without requiring face-to-face consultations, reducing hospital admission and avoiding unnecessary appointments.

To address the need for secure and reliable communications over WBANs, the IEEE developed the IEEE 802.15.6 international standard in 2012. This standard establishes key technical specifications for such systems, ensuring the integrity and confidentiality of data transmitted in the network while facilitating monitoring and control of sensor nodes (Salehi *et al.*, 2016).

As WBANs continue to evolve, they promise not only to revolutionize healthcare but also to create opportunities in diverse domains such as fitness, eldercare, and workplace safety. However, alongside these opportunities significant difficulties also arise in this field of research. Energy efficiency, security, and interoperability are closely tied to medical and regulatory aspects, posing complex challenges to overcome. Based on previous implementations and conducted experiments, this paper explores the current landscape of WBANs, highlighting key challenges and potential opportunities with a communication focused perspective and their role in an increasingly interconnected future. Although addressing legal aspects is critical in developing WBANs, particularly concerning medical use and data privacy of personal information, this work focuses on implementation challenges. An extensive discussion of regulations would exceed the intended scope of this analysis.

The remainder of this work is organized as follows: Section 2 gives a general overview about common WBAN frameworks and the most important communication standards in use. In Section 3 main challenges and associated complications that must be considered during development, implementation, and deployment are explored. Within Section 4 challenges of integrating the WBAN concept inside smart hospital environments in a future hyperconnected world is discussed based on current research and technological advancements. Finally, this work concludes in Section 5, which also provides an outlook on considerations for future research in this field.

2. Common Communication Standards Regarding WBANs

WBANs rely on different established communication standards and frameworks to ensure reliable data transmission and interoperability. This chapter explores the foundational aspects, starting with an overview of prevalent WBAN standards. Next, widely used communication standards and other significant frameworks are examined, highlighting their distinctive advantages regarding energy efficiency, range, and data throughput, along with their relevance for WBAN applications.

2.1 WBAN Standards

WBANs use wireless networks designed to facilitate communication among devices located on, in, or around the human body, primarily for healthcare applications. The IEEE 802.15.6-2012 standard was specifically developed to cater the unique requirements of WBANs. This standard provides essential specifications for low-power, short-range, and highly reliable communication in medical and healthcare applications. It addresses aspects such as security and device interoperability, ensuring the integrity and confidentiality of transmitted data. Although the original IEEE 802.15.6-2012 standard is no longer actively maintained, the IEEE 802.15.6ma Task Group is currently engaged in efforts to revise and extend its capabilities (Hernandez *et al.*, 2022). This initiative aims to address evolving requirements in WBANs and technological advancements by enhancing reliability, mitigating interference, and expanding the scope to include both Human Body Area Networks (HBANs) and Vehicle Body Area Networks (VBANs). These extensions are designed to support new use cases, such as seamless integration with Internet-of-Things (IoT) infrastructure, reliable communication in congested environments, and interoperability with emerging technologies like Beyond 5G, wireless technologies of the 6th generation (6G) and Time-Sensitive Networking (TSN). Thus, the standard should remain relevant and fulfil the growing requirements of the healthcare sector, automotive industry and other critical areas in the wider context of the internet.

In addition to this standard, there are also other dedicated endeavors. One such initiative is the Smart Body Area Network (SmartBAN) developed by the European Telecommunications Standards Institute (ETSI). SmartBAN prioritizes ultra-low-power and short-range communication, optimized specifically for BANs. It places a strong emphasis on interoperability and efficient coexistence with other wireless technologies, making it well-suited for healthcare monitoring and well-being applications (Hamalainen *et al.*, 2020).

Another significant framework is oneM2M, a global project to create a standardized service layer for seamless Machine-to-Machine and IoT communications. oneM2M provides common service functions and standardized interfaces, enabling interoperability among diverse devices and platforms. This framework supports the integration of WBANs into larger IoT ecosystems, ensuring that the benefits can be extended across various domains, including healthcare (Adriansyah and Amrullah, 2021).

Despite not being a standardization committee, the Alliance for IoT and Edge Computing Innovation (AIOTI) plays a crucial role in promoting the development and adoption of IoT solutions across Europe. AIOTI focuses on addressing challenges related to interoperability, standardization, and policy, thereby fostering the creation of a dynamic European IoT ecosystem that encompasses WBAN technologies.

These initiatives collectively address critical challenges arising from the limitations of the original IEEE 802.15.6 standard, ensuring the continued evolution of WBAN technologies. They focus on key areas such as interoperability, energy efficiency, and integration with IoT ecosystems, which are vital for advancing technology in healthcare and personal health monitoring. These efforts provide frameworks for seamless communication, efficient resource utilization, and coexistence with other wireless technologies. As a result, WBAN systems can adapt to meet modern demands, supporting applications ranging from clinical environments to personal well-being and beyond.

2.2 Communication Standards

2.2.1 Bluetooth and BLE (IEEE 802.15.1)

Bluetooth, standardized under IEEE 802.15.1, is a widely adopted short-range wireless communication protocol primarily used for connecting handheld devices. Operating in the 2.4 GHz ISM band, it employs frequency hopping across 79 channels with 1 MHz bandwidth at a rate of 1600 hops per second to minimize interference. Bluetooth devices typically function within a piconet, wherein one device assumes the role of the master while others serve as slaves throughout the duration of the connection. Synchronization is achieved via the master's clock. The classic Bluetooth version 2.0+ EDR (Enhanced Data Rate) supports a maximum data rate of 3 Mbps, making it suitable for applications requiring moderate bandwidth (Trelsmo *et al.*, 2017). A significant advancement is Bluetooth Low Energy (BLE), a distinct protocol designed for ultra-low-power applications. While it shares the same 2.4 GHz band, BLE uses a different communication mechanism with 40 channels within 2 MHz bandwidth and operates at a significantly lower power level. Thus, it is ideal for battery-powered devices in healthcare, fitness, and IoT applications. By prioritizing energy efficiency over data throughput, BLE supports data rates up to 1 Mbps and typically uses smaller data packets.

Although classic Bluetooth may consume considerable power, potentially reducing battery life in certain applications, its compatibility and robust features render it a preferred choice for high-bandwidth connections. BLE, on the other hand, excels in scenarios where low power consumption and intermittent data exchange are crucial, making it a preferred choice in wearable devices and wireless sensor networks.

2.2.2 ZigBee (IEEE 802.15.4)

ZigBee is a widely used method for low-power communication, designed to enable efficient and reliable wireless networking. It consumes approximately 60 mW of power and is optimized for devices requiring long battery life and operating in environments with limited energy resources. ZigBee is commonly employed in IoT applications, particularly in scenarios where collision avoidance is paramount. It supports a modest data rate of 250 kbps, which is adequate for transmitting small data packets over prolonged periods. Through its mesh networking capabilities, Zigbee enhances both network reliability and range. Applications include home automation, industrial control, smart metering, and environmental monitoring. Furthermore, ZigBee's ability to operate on unlicensed frequency bands and its strong security features make it a popular choice for cost-effective and secure IoT deployments (Tennina *et al.*, 2013).

2.2.3 Ultra-Wideband (UWB)

Ultra-Wideband (UWB) is a radio technology that operates over a wide frequency spectrum - typically 500 MHz or more - and is supported as one of the physical layers (PHY) in IEEE 802.15.6. UWB is renowned for its high data rates, low power consumption, and exceptional precision in location tracking, often complementing GPS in BAN applications. It is often used for real-time tracking and localization tasks in healthcare and IoT environments. Furthermore, UWB's wide bandwidth enhances its resilience to interference, enabling more reliable and efficient communication in crowded spectral environments (Cicchetti, Miozzi and Testa, 2017).

2.3 Further Notable Communication Frameworks

2.3.1 Human body communication (HBC)

IEEE 802.15.6 offers a specification for Human Body Communication (HBC) communication, which operates within the range of 10 MHz to 50 MHz for devices in WBANs. The band of operation is centered at 21 MHz (*IEEE Standard for Local and metropolitan area networks - Part 802.15.6: Wireless Body Area Networks*, no date). HBC is a technology that utilizes the human body as a medium for transmitting data between devices via capacitive, or galvanic coupling. In the context of capacitive coupling an electric field is induced exploiting the body's high water content to propagate electrical signals. The data rate can exceed 2 Mbps.

2.3.2 ANT and ANT+

ANT is a proprietary wireless communication protocol developed by Dynastream Innovations; a Canadian company acquired by Garmin in 2006. Operating in the 2.4 GHz ISM band, ANT is designed for ultra-low-power, short-range wireless communication, making it ideal for fitness and health monitoring applications. Its flexible network topologies, including star, mesh, and tree configurations, enable devices from various manufacturers to communicate seamlessly within a low-power wireless network. ANT+ serves as interoperability function built on top of the ANT protocol, facilitating this wide compatibility. This technology was often used for heart rate monitors, bike sensors, and fitness trackers, licensed by Garmin.

Despite its strengths, recent developments indicate a potential decline of ANT in the future. Garmin has announced to discontinue certification processes and development of new ANT+ standards, partly due to challenges posed by regulatory updates like the EU Radio Equipment Directive (EU RED)[1]. This directive mandates encryption and authentication for wireless communication involving personal information. Although ANT+ can meet these requirements, implementation would compromise backward compatibility with existing devices, discouraging manufacturers from continuing to adopt the technology.

2.3.3 Medical implant communication service (MICS):

Medical Implant Communication Service (MICS) is a specialized wireless communication standard operating in the 402 – 405 MHz frequency band, allocated globally by the International Telecommunication Union (ITU) for medical use. This ultra-low-power, short-range protocol is specifically designed for implantable medical devices, such as pacemakers and defibrillators, ensuring secure and reliable data transmission between implants and external monitoring or programming devices. MICS is heavily regulated to prevent interference with other systems and to maintain safety within human tissue. Its applications have expanded with advancements in healthcare technology, supporting the growing demand for remote monitoring and control of medical implants in clinical and personal healthcare environments (Jovanov and Milenkovic, 2011).

3. WBAN Challenges

WBANs are pivotal for healthcare and IoT applications. However, their development and implementation introduce significant interdisciplinary challenges, which are systematically explored in this chapter. First, implementation-related difficulties are addressed, along with associated complications and trade-offs to consider. Subsequently, the discussion shifts to another critical challenge in WBAN deployment: authentication mechanisms to ensure user privacy and security, and data integrity and confidentiality.

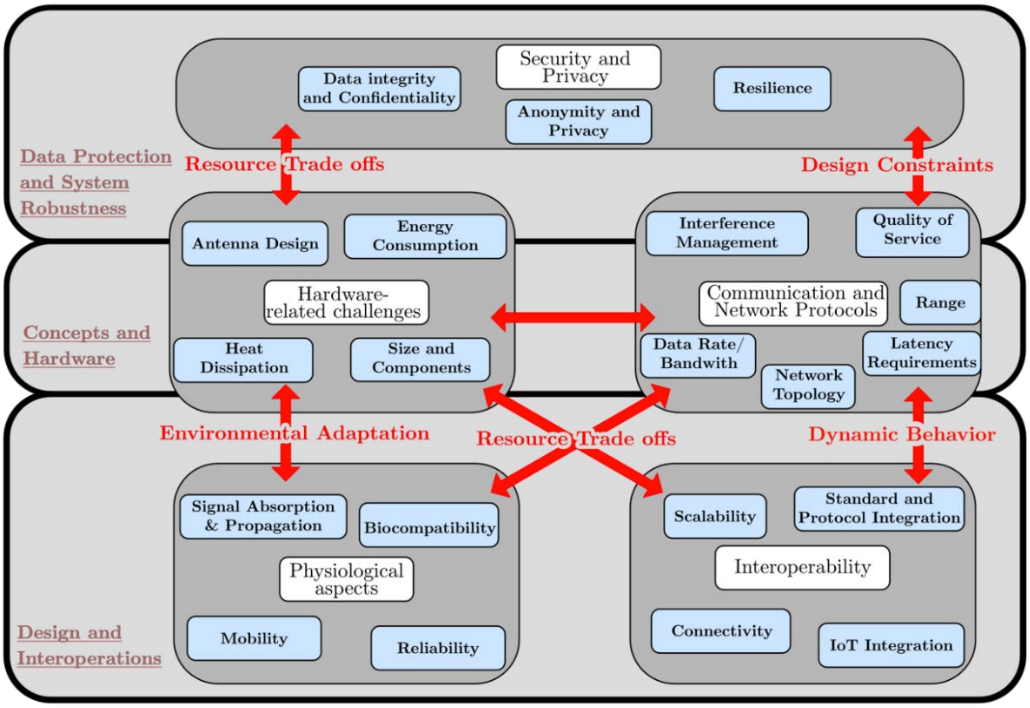

Figure 1: WBAN Challenge Model: Overview of identified challenging aspects with influencing dependencies to each other, embedded in a superordinate layer design

[1]https://www.thisisant.com/business/go-ant/ant-brand - 07.01.2025

3.1 Implementation Challenges

Based on previous hardware implementations (Herbst *et al.*, 2022; Herbst, Müller, *et al.*, 2024), challenges are identified and categorized into five main groups. Each group covers specific aspects demonstrating bidirectional influences on others, collectively impacting WBAN performance and usability. The areas themselves are organized in a superordinate layer design, which encompasses *Data Protection and System Robustness*, *Concepts and Hardware*, and *Design and Interoperations*. The identified challenge areas and their bidirectional influences are illustrated in Figure 1. The interconnected nature emphasizes the importance of a holistic approach for system design, where addressing one challenge must account for its potential effects across other domains. By leveraging insights from existing research and standards, including those related to WBAN technologies, designers must effectively navigate these complexities to ensure innovative and practical solutions.

A comprehensive overview of most important bidirectional influences from different areas are given in Table 1.

Table 1: Overview of most important bidirectional influences of different challenge categories in WBAN design

Aspect 1	Aspect 2	Influence	Affected Categories
Data Integrity	Size and Components	Secure Data Transmission	Security ↔ Hardware
Resilience	Antenna Design	Robustness in Design	Security ↔ Hardware
Anonymity	Interference Management	Privacy in Communication	Security ↔ Communication
Resilience	Network Topology	Reliable Communication Structures	Security ↔ Communication
Antenna Design	Signal Absorption	Performance Adaptation	Hardware ↔ Physiological
Energy Consumption	Mobility	Power Efficiency	Hardware ↔ Physiological
Energy Consumption	Latency + Bandwidth	Power Efficiency	Hardware ↔ Communication
Network Topology	Scalability	System Expansion	Communication ↔ Interoperability
Interference Management	Reliability	Signal Stability	Communication ↔ Physiological
Bandwidth	Signal Absorption	Data Throughput	Communication ↔ Physiological
Range	Signal Absorption	Reliable Transmission	Communication ↔ Physiological
Data Integrity	Biocompatibility	Safe Data Processing	Security ↔ Physiological
Anonymity	IoT Integration	Privacy in Connected Systems	Security ↔ Interoperability
Resilience	Signal Absorption	System Safety in Environmental Conditions	Security ↔ Physiological
Anonymity	Scalability	Privacy in Large Systems	Security ↔ Interoperability

3.1.1 *Security and privacy*

Security and privacy considerations are paramount in system design, focusing on protecting sensitive data and ensuring system robustness. Critical aspects include **confidentiality, data integrity, and availability (CIA)**, which safeguard information from unauthorized access and ensure its accuracy during transmission. Simultaneously, **anonymity and privacy** are essential to protect user identities and personal data from exploitation (Al-Janabi *et al.*, 2017). Additionally, **resilience** is emphasized, ensuring that the system can withstand and recover from potential threats or failures. Addressing these areas often leads to design constraints, as achieving strong security typically increases resource demands such as energy consumption and computational overhead (Djenouri and Balasingham, 2009) (Ojelade, Ibrahim and Ata, 2021).

3.1.2 *Hardware related challenges*

This area addresses the physical components and foundational design of systems, including **antenna design**, **energy consumption**, **heat dissipation**, and **size and compactness**. Optimizing antenna design is crucial for efficient signal transmission, while **energy consumption** must balance performance with power efficiency to ensure prolonged device operation (Romer and Mattern, 2004). Effective **heat dissipation** is necessary to maintain safety and comfort, particularly for wearable or implantable devices. These hardware elements are influenced by resource trade-offs, as improvements in one area (e.g., performance) may increase demands in another (e.g., energy or heat management) (Rubani *et al.*, 2019).

3.1.3 *Communication and Network Protocols*

Efficient communication is vital for advanced systems, with key considerations such as **data rate/bandwidth**, **interference management**, **network topology**, **latency requirements**, and **range**. Data throughput must support real-time applications without excessive resource demands, while interference management is critical in densely connected environments. Network topology must accommodate mobility and reduce latency, ensuring seamless connectivity across varying distances. This area is marked by dynamic behavior, as communication protocols must adapt to changes in the environment and user mobility while maintaining reliability and quality (Mile, Okeyo and Kibe, 2018; Ojelade, Ibrahim and Ata, 2021).

3.1.4 *Physiological Aspects*

Systems interacting with the human body must address **signal absorption and propagation**, **mobility**, **biocompatibility**, and **reliability**. Signal absorption is affected by the dielectric properties of human tissue, which can degrade signal quality and connectivity. Mobility introduces dynamic changes in body position and motion, requiring robust protocols to maintain communication. Biocompatibility ensures that materials and device designs are safe and comfortable for users, while reliability guarantees consistent performance under varying physiological conditions. These aspects demand **environmental adaptation**, where systems must dynamically adjust to the human body's unique properties and behavior (Mile, Okeyo and Kibe, 2018; Rubani *et al.*, 2019).

3.1.5 *Interoperability*

This area focuses on the integration of systems into larger ecosystems, highlighting **scalability**, **standard and protocol integration**, **interoperability**, **connectivity**, and **IoT integration**. Scalability ensures that systems can expand without compromising performance, while interoperability and standardization facilitate seamless integration across devices and networks. Connectivity and IoT integration allow systems to operate within broader IoT infrastructures, enabling data sharing and advanced applications. These components require careful management of **resource trade-offs**, as increasing scalability or IoT integration may strain energy resources, interference or latency requirements (Romer and Mattern, 2004; Djenouri and Balasingham, 2009).

3.2 Authentication Challenges

Ensuring the privacy and security of data is paramount, particularly in systems handling sensitive medical and body-near data of individuals. To preserve confidentiality and maintain data integrity of health-related information that is accessed, transmitted, and processed in WBANs, robust measures must be implemented to shield this data from unauthorized access, thereby protecting user privacy.

Various methods are available for verifying user identity in WBAN systems, ranging from key-exchange protocols and smartcards containing hash-codes to Physical Unclonable Functions (PUFs) that ensure system integrity. Within the diverse landscape of verification schemes, biometric-based authentication emerges as a particularly promising approach, considering the intrinsic existing data availability. Already prevalent in everyday devices like smartphones, laptops, and other IoT-enabled systems, biometric authentication leverages unique physiological or behavioral traits of individuals to provide secure and reliable user verification. For instance, identity can be confirmed through analysis of electrocardiography (ECG) patterns or gait characteristics (Lipps *et al.*, 2022; Herbst, Bergkemper and Lipps, 2023).

WBAN systems can extend this concept by intrinsically learning an individual's characteristics through the integrated sensors, including Inertial Measurement Units (IMUs), ECG devices, and all other kinds of wearable health-monitoring sensory. This paves the way for sophisticated Multi-Factor Authentication (MFA) that combines biometrics with context-aware methods, such as location and activity recognition, enabling continuous authentication (Herbst *et al.*, 2022).

Such systems can dynamically verify user identity, enhancing security while reducing dependency on static credentials like passwords or tokens. Biometric and context-aware authentication offers seamless and non-intrusive user experience while being inherently tied to an individual, making it difficult to forge. Continuous authentication further adds a layer of dynamic security, ensuring that the WBAN remains accessible only to the intended user even under changing circumstances.

However, these methods also face significant challenges. Biometric systems can be susceptible to noise and environmental factors, potentially reducing accuracy. In addition, continuous authentication requires constant data acquisition and processing, which adds challenges regarding energy and computational resources of WBAN devices. Furthermore, the reliability of context-aware systems hinges on data quality (depending on quality and reliability of sensors and their positioning) and robustness of the algorithms used for recognition. Major concerns in biometric authentication revolves around privacy, given that biometric data is immutable. If such data is compromised, it could have long-lasting implications. Therefore, data integrity and security of this sensitive information is of utmost priority. To achieve this, robust cryptographic algorithms are essential. One promising technology in this regard is homomorphic encryption.

A detailed analysis of various security mechanisms is available in (Herbst, Rüb, *et al.*, 2024), as further discussion would exceed the scope of this work, constituting a topic in its own right.

Despite these challenges, a combination of biometric-based authentication, MFA, and context-aware mechanisms represents a significant step forward for verification in WBAN systems, providing a balance between security, usability, and adaptability. Future research should focus on refining these solutions to mitigate their limitations harnessing their inherent strengths. The aim is to develop robust and energy-efficient authentication frameworks for WBANs.

4. WBAN Challenges in Smart Hospital Context

The integration of WBANs within smart hospital environments as human-centric IoT systems offers a substantial promise for improving patient care. These systems can provide continuous data about a patient's health status in real-time, facilitating personalized treatment and more effective decision-making. To begin with, this chapter explores various cybersecurity threats that hospitals already face today and proposes strategies to counteract these, emphasizing the importance of awareness about cybersecurity in the increasingly digitized health sector. Thereafter incorporation of WBANs into smart hospital environments and resulting challenges along with potential solutions are discussed.

4.1 Cybersecurity Threats in Hospitals

Hospitals face a wide range of cybersecurity threats that can severely impact patient care, confidentiality, data security, and operational continuity. These threats include phishing attacks, ransomware, insider threats, device loss or theft, insecure data transmission, Distributed Denial-of-Service (DDoS) attacks (Syed *et al.*, 2020), and vulnerabilities in medical devices. Such risks emphasize the need for comprehensive cybersecurity strategies to ensure CIA of critical healthcare systems and sensitive data. To address these challenges, hospitals must implement robust and multilayered security measures. Firewalls and Intrusion Detection Systems (IDSs) are pivotal in monitoring and controlling network traffic, detecting unauthorized access attempts, and preventing malicious activities (Mishra and Pandya, 2021). These tools form a first line of defense against cyber intrusions and provide visibility into potential threats. Advanced encryption protocols, such as TLS 1.3, ensure the secure transmission of sensitive data between central servers and connected IoT devices (Paris, Habaebi and Zyoud, 2023, p. 202).

MFA mechanisms further support access control, reducing the risk of credential theft or misuse. Additionally, network segmentation is an essential strategy in high-risk environments. By isolating IoT systems from core hospital networks, network segmentation helps in containing potential threats and prevents them from spreading across the entire infrastructure. Proactive lifecycle management of IoT devices is another key element of hospital cybersecurity. Implementing strict patch management policies ensures that devices operate on the most recent firmware versions, thereby mitigating known vulnerabilities. For legacy devices that are no longer supported by manufacturers, alternative security measures, such as virtual patching through network appliances, can be employed to enhance security. Human factors also play a critical role in overall hospital cybersecurity. Regular training programs are essential for equipping healthcare staff with the skills to recognize phishing attempts, securely manage credentials, and comply to data protection protocols. Furthermore, comprehensive incident response plans are fundamental for enabling swift and effective action in the event of a security breach, minimizing potential damage and recovery time (Yuce, 2010).

4.2 WBANs in Smart Hospital Environments

A key benefit of WBANs is their capability to offer continuous information about an individual's health status, even prior to hospital admission. Patients equipped with WBAN devices can provide a history of health data, such as trends in heart rate, glucose levels, or physical activity. This continuity of information can reduce the dependency on isolated snapshots from conventional hospital monitoring and offers a more comprehensive context for individualized diagnosis and treatment. However, the incorporating patient-owned WBANs into a hospital's infrastructure poses difficulties on its own. Interoperability between personal WBANs and hospital systems for instance is not guaranteed. Therefore, the adoption of unified communication standards or protocols is important. Nevertheless, establishing universal standards and ensuring seamless integration will require significant effort and investment.

A particularly acute challenge in integrating WBANs into hospital networks are cybersecurity risks associated with this process. Patient-owned devices may introduce vulnerabilities into hospital systems, including outdated firmware, weak encryption, or unpatched security deficiencies. Such risks are magnified in environments where multiple IoT devices share the same infrastructure. To mitigate these risks, hospitals must implement robust network segmentation to isolate WBANs from core systems and employ advanced encryption protocols to secure data transmission. Additionally, real-time intrusion detection systems are essential to identify and respond to potential threats before they compromise patient data or system integrity.

Another challenge originates from balancing the continuous operation of WBANs with their resource constraints. These systems are designed to operate on minimal power, yet hospital environments often require handling intensive data transmission, leading to potential battery depletion or signal degradation of WBAN devices. Adaptive protocols that optimize the balance data transmission frequency and bandwidth with power efficiency will be crucial. Hospitals must also provide infrastructure for recharging or maintaining WBAN devices during extended admission.

Also from a privacy perspective, the use of personal WBANs introduces complexity to hospital infrastructure. While continuous monitoring enhances individualized care, it also generates a vast amount of sensitive personal data. Ensuring that this data is used responsibly and remains accessible only to authorized personnel is critical. Biometric-based authentication, such as the use of ECG patterns, offers a promising solution for securing WBAN systems. Ensuring that these methods are robust against spoofing attempts and effective in minimizing false positives is essential for maintaining security and confidentiality. Moreover, privacy concerns extend to how data is shared between hospitals, patients, and external systems, requiring clear policies and technical safeguards.

Despite these challenges, the integration of WBANs into smart hospital environments offers transformative possibilities. Continuous data provided by WBANs can facilitate predictive analytics, allowing Machine Learning algorithms to detect early indicators of critical conditions such as sepsis or cardiac events. Real-time insights can reduce the necessity of invasive procedures and lower hospital readmissions by offering targeted and timely interventions. Hospitals also could extend patient care beyond their physical facilities: remote monitoring can continue for patients who have been discharged wearing their WBAN systems, allowing for smooth transitions from hospital care to home recovery. Alerts for complications, such as post-surgical infections, can prompt early interventions, thereby improving recovery and reducing healthcare costs. However, during this phase, it is essential for WBAN systems to remain secure, functional, and compatible with telemedicine platforms.

5. Conclusion and Future Work

Integrating Wireless Body Area Networks (WBANs) into smart hospital environments can represent a paradigm shift to revolutionize healthcare by offering opportunities for continuous, individualized, and data-driven healthcare. However, this potential interconnected future is occupied with significant challenges, particularly concerning interoperability, cybersecurity, resource efficiency, and privacy. This work presents an in-depth exploration of these challenges.

With an overview of existing WBAN standards significant efforts have been explored to foster advancements of WBAN technologies, pushing beyond the constraints of the original IEEE 802.15.6-2012 WBAN standard to ensure reliable data transmission and interoperability in the future. A discourse on existing communication protocols, and standards used for Internet of Things (IoT) and WBAN systems has elucidated their respective strengths and limitations. The relevance of communication standards, such as Bluetooth, Zigbee, and Medical Implant Communication Service (MICS), for future WBAN systems has been elaborated based on range, bandwidth and energy efficiency.

The development and implementation of WBAN systems are complex and interdisciplinary tasks, highlighted by identification of five key challenge areas that interact and require balancing trade-offs. These areas — “Security and Privacy”, “Hardware-related Challenges”, “Communication and Network Protocols”, “Physiological Aspects”, and “Interoperability” — have been thoroughly investigated. The focus on data privacy underscores the essential requirement for secure and reliable data acquisition, processing, and transmission. Authentication is crucial for safeguarding WBANs against unauthorized access and ensuring confidentiality and user privacy. Various existing authentication schemes have been reviewed, with a combination of contextual and biometric authentication emerging as a particularly promising approach, despite its own challenges related to the use of an individuals’ inherent physiological or behavioral characteristics.

Incorporating WBAN systems within a smart hospital environment introduces additional difficulties. Key considerations extend beyond data privacy and security of single WBANs to encompass cybersecurity and overall integrity of hospital infrastructure. Threats already existing today, and their corresponding mitigation strategies have been analyzed and projected to the integration of WBAN systems. The primary challenges identified for this integration include interoperability, confidentiality, functionality, and mitigating vulnerabilities within both the WBAN technologies and hospital infrastructure.

By addressing these obstacles, hospitals can leverage the full potential of WBANs to enhance care while safeguarding patient trust, data privacy, and system integrity. Realizing this vision will require collaborative efforts across technology, legal frameworks, and clinical practice, ensuring that all involved parties benefit equally from the advancements.

Acknowledgement

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16KISK214, 6G-Health and 16KISK003K, Open6GHub). The authors alone are responsible for the content of the paper.

References

Adriansyah, A. and Amrullah, A.G. (2021) ‘Design of Health Monitoring Framework Model using oneM2M Standard’, *International Journal of Electrical, Energy and Power System Engineering*, 4(1), pp. 107–112. Available at: https://doi.org/10.31258/ijeepse.4.1.107-112.

Al-Janabi, S. *et al.* (2017) ‘Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications’, *Egyptian Informatics Journal*, 18(2), pp. 113–122. Available at: https://doi.org/10.1016/j.eij.2016.11.001.

Cicchetti, R., Miozzi, E. and Testa, O. (2017) ‘Wideband and UWB Antennas for Wireless Applications: A Comprehensive Review’, *International Journal of Antennas and Propagation*, 2017, pp. 1–45. Available at: https://doi.org/10.1155/2017/2390808.

Djenouri, D. and Balasingham, I. (2009) ‘New QoS and Geographical Routing in Wireless Biomedical Sensor Networks’, in *Proceedings of the 6th International ICST Conference on Broadband Communications, Networks, and Systems*. *6th International ICST Conference on Broadband Communications, Networks, and Systems*, Madrid, Spain: IEEE. Available at: https://doi.org/10.4108/ICST.BROADNETS2009.7188.

Hamalainen, M. *et al.* (2020) ‘ETSI SmartBAN Architecture: The Global Vision for Smart Body Area Networks’, *IEEE Access*, 8, pp. 150611–150625. Available at: https://doi.org/10.1109/ACCESS.2020.3016705.

Herbst, J. *et al.* (2022) ‘Body Area Networks in the Era of 6G: An Evaluation of Modern Biometrics regarding Multi-Factor-Authentication’, in. *Next Generation Networks and Applications (NGNA)*. Available at: http://dx.doi.org/10.13140/RG.2.2.18435.17449.

Herbst, J., Müller, R., *et al.* (2024) ‘A Ring Topology Approach: Efficient Communication in Wireless Body Area Networks (WBANs)’, in *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, Antwerp, Belgium: IEEE, pp. 1084–1089. Available at: https://doi.org/10.1109/EuCNC/6GSummit60053.2024.10597045.

Herbst, J., Rüb, M., *et al.* (2024) ‘Medical Data in Wireless Body Area Networks: Device Authentication Techniques and Threat Mitigation Strategies Based on a Token-Based Communication Approach’, *Network*, 4(2), pp. 133–149. Available at: https://doi.org/10.3390/network4020007.

Herbst, J., Bergkemper, L. and Lipps, C. (2023) 'Step by Step: A Gait-Centric Approach to Footbed-Based Recognition', *Next Generation Networks and Applications (NGNA)* [Preprint].

Hernandez, M. *et al.* (2022) 'New Revision of IEEE 802.15.6 Wireless Body Area Networks', in *2022 IEEE 16th International Symposium on Medical Information and Communication Technology (ISMICT)*. *2022 IEEE 16th International Symposium on Medical Information and Communication Technology (ISMICT)*, Lincoln, NE, USA: IEEE, pp. 1–5. Available at: https://doi.org/10.1109/ISMICT56646.2022.9828139.

IEEE Standard for Local and metropolitan area networks - Part 802.15.6: Wireless Body Area Networks (no date). IEEE. Available at: https://doi.org/10.1109/IEEESTD.2012.6161600.

Jovanov, E. and Milenkovic, A. (2011) 'Body Area Networks for Ubiquitous Healthcare Applications: Opportunities and Challenges', *Journal of Medical Systems*, 35(5), pp. 1245–1254. Available at: https://doi.org/10.1007/s10916-011-9661-x.

Lipps, C. *et al.* (2022) 'I Know You by Heart: Biometric Authentication based on Electrocardiogram (ECG) signals', *International Conference on Cyber Warfare and Security*, 17(1), pp. 135–144. Available at: https://doi.org/10.34190/iccws.17.1.12.

Mackay, R.S. (1959) 'Radio Telemetering from Within the Human Body', *IRE Transactions on Medical Electronics*, ME-6(2), pp. 100–105. Available at: https://doi.org/10.1109/IRET-ME.1959.5007926.

Mile, A., Okeyo, G. and Kibe, A. (2018) 'Hybrid IEEE 802.15.6 Wireless Body Area Networks Interference Mitigation Model for High Mobility Interference Scenarios', *Wireless Engineering and Technology*, 09(02), pp. 34–48. Available at: https://doi.org/10.4236/wet.2018.92004.

Mishra, N. and Pandya, S. (2021) 'Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review', *IEEE Access*, 9, pp. 59353–59377. Available at: https://doi.org/10.1109/ACCESS.2021.3073408.

Ojelade, A.K., Ibrahim, A.A. and Ata, O. (2021) 'Efficient Energy and QoS Based Routing Algorithm for Wireless Body Area Network', in *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Ankara, Turkey: IEEE, pp. 110–115. Available at: https://doi.org/10.1109/ISMSIT52890.2021.9604714.

Paris, I.L.B.M., Habaebi, M.H. and Zyoud, A.M. (2023) 'Implementation of SSL/TLS Security with MQTT Protocol in IoT Environment', *Wireless Personal Communications*, 132(1), pp. 163–182. Available at: https://doi.org/10.1007/s11277-023-10605-y.

Preethichandra, D.M.G. *et al.* (2023) 'Wireless Body Area Networks and Their Applications—A Review', *IEEE Access*, 11, pp. 9202–9220. Available at: https://doi.org/10.1109/ACCESS.2023.3239008.

Romer, K. and Mattern, F. (2004) 'The design space of wireless sensor networks', *IEEE Wireless Communications*, 11(6), pp. 54–61. Available at: https://doi.org/10.1109/MWC.2004.1368897.

Rubani, Q. *et al.* (2019) 'Design and analysis of a terahertz antenna for wireless body area networks', *Optik*, 179, pp. 684–690. Available at: https://doi.org/10.1016/j.ijleo.2018.10.202.

Salehi, S.A. *et al.* (2016) 'IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view', in *2016 22nd Asia-Pacific Conference on Communications (APCC)*. *2016 22nd Asia-Pacific Conference on Communications (APCC)*, Yogyakarta, Indonesia: IEEE, pp. 523–528. Available at: https://doi.org/10.1109/APCC.2016.7581523.

Syed, N.F. *et al.* (2020) 'Denial of service attack detection through machine learning for the IoT', *Journal of Information and Telecommunication*, 4(4), pp. 482–503. Available at: https://doi.org/10.1080/24751839.2020.1767484.

Tennina, S. *et al.* (2013) *IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints*. Berlin, Heidelberg: Springer Berlin Heidelberg (SpringerBriefs in Electrical and Computer Engineering). Available at: https://doi.org/10.1007/978-3-642-37368-8.

Trelsmo, P. *et al.* (2017) 'Evaluating IPv6 Connectivity for IEEE 802.15.4 and Bluetooth Low Energy', in *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, San Francisco, CA, USA: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/WCNCW.2017.7919088.

Yuce, M.R. (2010) 'Implementation of wireless body area networks for healthcare systems', *Sensors and Actuators A: Physical*, 162(1), pp. 116–129. Available at: https://doi.org/10.1016/j.sna.2010.06.004.

Zimmerman, T.G. (1996) 'Personal Area Networks: Near-field intrabody communication', *IBM Systems Journal*, 35(3.4), pp. 609–617. Available at: https://doi.org/10.1147/sj.353.0609.